UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/994,476	11/26/2001	Ari Juels	RSA-502AUS	7236

22494 7590 03/15/2006

DALY, CROWLEY, MOFFORD & DURKEE, LLP
SUITE 301A
354A TURNPIKE STREET
CANTON, MA 02021-2714

EXAMINER	
WILLIAMS, JEFFERY L	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 03/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/994,476	JUELS ET AL.	
	Examiner	Art Unit	
	Jeffery Williams	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28 and 38-45* is/are pending in the application.

4a) Of the above claim(s) *29-37* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28 and 38-45* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *04 March 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the communication filed on 12/12/2005.

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 2, 4 – 17, 19 – 28, and 40 – 45 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. These claims have been amended to include "computer implemented" within the preamble. The examiner kindly points out that whether a method includes "computer implemented" or not, is immaterial to making a determination as to whether the subject matter is patent-eligible. Regarding the above claims, the claim language is directed to a method of computation wherein no tangible result is provided. Thus, the claims do not result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 U.S.C. 101.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1 – 3, 6 – 9, 11, 12, 14 – 17, 19 – 23, 26 – 28, and 38 – 44 are rejected under 35 U.S.C. 102(b) as being anticipated by Alabbadi et al., "Integrated Security and Error Control for Communication Networks Using the McEliece Cryptosystem".

Regarding claim 19, Alabbadi et al. discloses:

receiving a first set of elements (Alabbadi; page 2, col. 1, "Encryption and encoding": Step 2);

and selecting a polynomial for encoding the item under the first set of elements to generate an order-invariant fuzzy commitment of the item (Alabbadi; page 2, col. 1, "Encryption and encoding": Step 3; page 1, col. 2, par. 3). Alabbadi discloses creating a commitment through the use of the polynomial despite when it would appear that the order of the elements has varied due to the introduction of bit errors.

Regarding claim 20, Alabbadi et al. discloses:

further including inserting chaff points that form a part of the commitment of the item (Alabbadi; page 1, col. 2, par. 2).

Regarding claim 21, Alabbadi et al. discloses:

receiving a second set of elements (Alabbadi, page 2, col. 1, "Encryption and encoding": Step 4 – "Decryption and decoding": Step 1); *and selectively decommitting the item based upon a level of overlap of the first and second sets of elements* (Alabbadi, page 2, col. 1, "Decryption and decoding": Step 2).

Regarding claim 22, Alabbadi et al. discloses:

further including determining the polynomial from the second set of elements if the level of overlap is greater than a predetermined threshold (Alabbadi, page 2, col. 1, "Setup": Step 1).

Regarding claim 23, Alabbadi et al. discloses:

further utilizing an error-correcting code for determining the polynomial (Alabbadi; page 1, col. 2, par. 3).

Regarding claim 26, Alabbadi et al. discloses:

further including utilizing a decodable design to decommit the item, wherein the decodable design includes constituent pairs of sets having a level of overlap less than a predetermined level (see rejections for claims 21 and 22).

Regarding claim 27, Alabbadi et al. discloses:

further including hiding the first set of elements in a target set containing a plurality of elements selected from a field (Alabbadi, page 1, col. 2, par. 2; "Encryption and encoding": Step 3).

Regarding claim 28, Alabbadi et al. discloses:

further including projecting the first set of elements onto the target set (Alabbadi, page 1, col. 2, par. 2; "Encryption and encoding": Step 3).

Regarding claim 1, Alabbadi et al. discloses:

(a) receiving a first input element comprising a sequence of a least one value $(a_1,\ldots, a_n)$ *from a predetermined set* (Alabbadi; page 2, col. 1, "Encryption and encoding": Step 2). Alabbadi et al. discloses receiving an input comprising a sequence of 'm' vectors from a predetermined set of 'M'.

(b) generating a codeword of an error-correcting code for generating the commitment (Alabbadi; page 1, col. 2, par. 3; page 2, col. 1, "Setup": Step 1).

(c) constructing a first sequence of coordinate sets (x_i, y_i), *for i in {1,...n}, each of the coordinate sets having a first value* (x_i) *corresponding to a representation of an associated one* (a_i) *of the at least one value of the first input element and a second value* (y_i) *corresponding to a symbol in the codeword, wherein the symbol corresponds to the* x_i*th symbol in the codeword, wherein an order-invariant fuzzy commitment is*

formed (Alabbadi; page 1, col. 2, par. 3; page 2, col. 1, "Setup": Step 1; page 2, col. 1, "Encryption and encoding": Step 3;). Alabbadi et al. discloses that the input elements and their corresponding symbols in the codeword are mapped (committed) using a two dimensional matrix, thus creating the equivalent of the claimed "coordinate sets". The commitment is created despite when it would appear that the order of the elements has varied due to the introduction of bit errors.

Regarding claim 2, Alabbadi et al. discloses:

wherein the representation of the first value in the first sequence of coordinate set is an integer representation (Alabbadi; page 2, col. 1, "Encryption and encoding": Step 2). Alabbadi et al. discloses the first value to be a k – bit vector, or bit sequence.

Regarding claim 3, Alabbadi et al. discloses:

further including outputting the first sequence (Alabbadi, page 1, col. 2, par. 2; "Encryption and encoding": Step 4).

Regarding claim 6, it is rejected for the same reasons as claim 20.

Regarding claim 7, Alabbadi et al. discloses:

further including adding the chaff as sets of pairs of the form (x,y) such that x does not lie in the input sequence and y is generated at random (Alabbadi; page 1, col. 2, par. 2; page 2, col. 1, "Encryption and encoding": Step 4). Alabbadi et al. discloses the input of pairs of "chaff" elements. X representing intentional user errors of which do

not lie in the input sequence, and Y representing channel noise occurring accidentally (random).

Regarding claim 8, Alabbadi et al. discloses:

further including adding the chaff as sets of pairs of the form (x,y) such that one or more values x do lie in the input sequence and y is generated at random (Alabbadi; page 1, col. 2, par. 7).

Regarding claim 9, Alabbadi et al. discloses:

further including reordering the first sequence based upon the first value (Alabbadi; page 2, col. 1, "Setup": Step 2). The first sequence in relation to the first value has been reordered via the permutation matrix.

Regarding claim 11, Alabbadi et al. discloses:

further including applying a bijective function to an input secret to obtain the codeword for the symbol corresponding to the second value (Alabbadi; page 2, col. 1, "Encryption and encoding": Step 3).

Regarding claim 12, the combination of Alabbadi et al. and Davida et al. disclose:

receiving the first sequence (Alabbadi; page 2, col. 1, "Encryption and encoding": Step 2; Davida et al., page 1, col. 1, Introduction; page 1, col. 2; pages 5, 7, and 8);

selecting a subset of the coordinate sets {(xi, yi)} in the first sequence (E) such that for each pair (x', y') in the subset, the first value in the pair (x') lies in the derived set

of values (X') (Alabbadi; page 1, col. 2, par. 3; page 2, col. 1, "Setup": Step 1; page 2, col. 1, "Encryption and encoding": Step 3;). Alabbadi et al. discloses that the input elements and their corresponding symbols in the codeword are mapped (committed) using a two dimensional matrix, thus creating the equivalent of the claimed "coordinate sets";

receiving a second input element including a second sequence of a least one value ($b_1,\ldots, b_m$) from the predetermined set (Alabbadi; page 2, col. 1, "Encryption and encoding": Step 2; Davida et al., page 1, col. 1, Introduction; page 1, col. 2; pages 5, 7, and 8). The combination of Alabbadi et al. and Davida et al. show this second sequence to be the subsequent (after storing a biometric template during initialization) entry by the user of biometric data so as to authenticate himself to the system.

constructing a derived set of values ($X'= x_1',\ldots, x_{m'}$) representing respectively the at least one value ($b_1,\ldots, b_m$) in the second sequence (Alabbadi; page 2, col. 1, "Setup": Step 1; page 2, col. 1, "Encryption and encoding": Step 3). The combination of Alabbadi et al. and Davida et al. discloses that the input elements and their corresponding symbols in the codeword are mapped (committed) using a two dimensional matrix, thus creating the equivalent of coordinate sets.

applying an error-correcting function to the subset (Alabbadi; page 2, col. 1, "Encryption and encoding": Step 3).

Regarding claim 14, it is rejected for the same reasons as claim 19.

Regarding claims 15 and 16, they are rejected for the same reasons as claim 26.

Regarding claim 17, it is rejected for the same reasons as claim 12.

Regarding claims 38 and 39, they are the computer readable medium embodying the code to implement the method of claims 1 and 12, and they are rejected for the same reasons as claims 1 and 12.

Regarding claim 40, it is rejected for the same reasons as claim 1.

Regarding claims 41, 42, 43, and 44, they contain limitations similar to claims 1 and 12 with the additional limitation of *"constructing a first sequence (E) of coordinate sets* $(x_i, z_{i,}, y_i)$*"* with z_i being *"a second value* (z_i) *constructed in a manner responsive to a pattern of occurrence of the associated one* (a_i) *of the at least one value of the first input element"*. Thus claims 41, 42, 43, and 44, are rejected for the same reasons as claims 1 and 12, and further because Alabbadi et al. discloses the construction of a "coordinate set" comprising a second value (z_i). This second value is provided by the user for each element (m_i) of the first input sequence.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Alabbadi et al.

Regarding claim 10, Alabbadi et al. discloses a method of reordering the first sequence based upon the first value (Alabbadi; page 2, col. 1, "Setup": Step 2). Randomly reordering the sequence would provide a level of obfuscation. Alabaddi does not disclose that the reordering is in ascending order based upon the first value.

However, it would have been obvious to one of ordinary skill in the art to recognize that various methods of reordering the sequence could be used, such as reordering in ascending order. This would be obvious because one of ordinary skill in the art would have been motivated to provide a level of obfuscation to the original sequence and a technique such as reordering in ascending order would accomplish this.

Claims 13 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alabbadi et al. in view of Rao et al., "Private-Key Algebraic-Code Encryptions".

Regarding claim 24, Alabbadi et al. discloses the use of Goppa codes. However, Rao et al. discloses that this causes the system to become susceptible to attacks.

Rao et al. shows that one approach to prevent attacks is to use Reed – Solomon Codes instead.

Thus, it would have been obvious to one of ordinary skill in the art to employ the teaching of Rao et al. for utilizing a Reed-Solomon error detecting code in the system of Alabbadi et al. This would have been obvious because one of ordinary skill in the art would have been motivated to prevent attacks that would have resulted from employing a Goppa error detecting code.

Regarding claim 13, it is rejected for the same reasons as claim 24.

Claims 4, 5, 25, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Alabbadi et al. in view of Davida et al., "On Enabling Secure Applications Through Off-Line Biometric Identification".

Regarding the following claims, Alabbadi et al. discloses a method of employing error correction within communication networks for the purpose of authenticating users to such networks (Alabbadi et al., page 1, "Introduction").

Davida et al. also discloses a method for employing error correction within a communication network for authenticating users to the network. For the purpose of increased security, Davida et al. discloses that it is advantageous to authenticate a user

to such networks using the biometric data of the user, such as fingerprint, retinal scan, or iris scan information. In order to utilize the biometric data, Davida et al. discloses that potential users to the system must input a set a biometric data in the form of a biometric template. Then, upon a request for authorization, a user will supply to the system a second set of biometric data that will be compared to the template, the first set (Davida et al., page 1, col. 1, Introduction; page 1, col. 2; pages 5, 7, and 8).

It would have been obvious to one of ordinary skill in the art to employ the method of Davida et al. for supplying a biometric template within the system of Alabbadi et al. for authenticating a user to a communications network. This would have been obvious because one of ordinary skill in the art would have been motivated to provide increased security via the utilization of biometric data for authenticating users to a communications network.

Regarding claim 25, the combination of Alabbadi et al. and Davida et al. disclose: *wherein the first set of elements corresponds to a biometric template* (Davida et al., page 1, col. 1, Introduction; page 1, col. 2; pages 5, 7, and 8).

Regarding claims 4 and 5, they are rejected for the same reason as 25.

Regarding claim 45, it contains limitations similar to claims 1, 12, 41, 42, 43, and 44. However, the combination of Alabbadi et al. and Davida et al. does not disclose the

receiving of a first input comprising two values, each value being derived from a separate predetermined set of values.

However, the combination of Alabbadi et al. and Davida et al. does disclose that a system for authenticating a using biometrics may use multiple types of biometrics. The combination discloses that a persons "biometric" for some biometric systems would comprise a iris scan and a finger scan (Davida; page 2, par.3; page 3, par. 5). Thus, the combination of Alabbadi et al. and Davida et al., suggests utilizing multiple types of biometrics to be entered by a user.

It would have been obvious to one of ordinary skill in the art to utilize in a biometric authentication system the receiving of a first input comprising two values, each value being derived from a separate predetermined set of values. The two values specifically being derived from a separate predetermined set of biometric values, such as an value for a fingerprint scan and a value for an iris scan. This would have been obvious because one of ordinary skill in the art would have been motivated to utilize authentication inputs comprising two biometric values so as to increase the system's security with unique identification.

Response to Arguments

Applicant's arguments filed 12/12/2005 have been fully considered but they are not persuasive.

Applicant's argue primarily that:

I. *Applicant submits that Alabbadi is quite different from the claimed invention. Alabbadi does not teach commitment of a message and is not relevant to order invariance as claimed by Applicant.* (Remarks, pg. 1).

In response, the examiner points out that the reference of Alabbadi is clear in directing the readers' attention to the use and protection of messages. Additionally, the examiner notes that the arguments of the applicant's representative appear to be based on the fact that Alabbadi discloses the use of a public and private key. Thus, according to the applicant's representative, such would not constitute a commitment. However, the examiner points out that the applicant's representative provides no adequate basis for the assertion that a commitment is not formed because an asymmetric key was used.

II. *In contrast, Alabbadi teaches that a message m is encrypted under a public key PK; a second party needs a private key SK in order to recover the message m, where SK differs from PK. This is in contrast the invention as claimed which requires creating an order-invariant commitment of a predetermined set of values.* (Remarks, pg. 2)

The applicant argues the use of an asymmetric key by the prior art. Again, however, the examiner kindly points out that the applicant's representative provides no adequate basis for the assertion that Alabbadi does not teach a commitment.

III. *Further, Alabbadi does not even remotely teach decommitment made selectively on the basis of overlap between the transmitted message c and received message c'. The receiver does not know a priori what the degree of overlap is, and therefore cannot perform the operation selectively. Instead, the receiver in Alabbadi always executes the decryption operation, which succeeds only if the transmitted message c and received message c' are sufficiently similar, i.e., meet an error threshold.* (Remarks, pg. 2)

In response, the examiner points out that Alabbadi discloses that the receiver selects the bits for the decryption operation, wherein there exists a level of overlap. Furthermore, in response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the receiver knows *a priori what the degree of overlap is*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

IV. *While the system of Alabbadi may tolerate a certain, limited re-ordering of message elements such as by treating any reordered elements as errors, Alabbadi*

does not teach order invariance as claimed. For example, if the original message is (A,B,C,D,E), then received message (B,A,C,D,E) may be viewed as equivalent to the first message, but with 40% erroneous elements since two of the five elements (A and B) are out of order in the received message as compared to the original message. However, inserting errors into a ciphertext as taught by Alabbadi is completely different than order invariance as claimed. (Remarks, pg. 3)

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

V. *Applicant submits that certain dependent claims are further patentably distinguishable over the cited references. For example, claim 6 requires adding chaff to the first sequence. In the McEliece scheme and Alabbadi schemes, a message is converted into a codeword and then perturbed, i.e., errors are introduced. This is completely different than adding chaff to the first sequence as claimed.* (Remarks, pg. 3)

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffery Williams whose telephone number is (571) 272-7965. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jeffery Williams
AU: 2137

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER